UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/921,231	07/31/2001	Brian J. Matt	NA01-00101	6007

28875 7590 06/06/2006

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/921,231	MATT, BRIAN J.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,8-18 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,8-18 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A response to the Notice of Non-Compliant Amendment (mailed 03 March 2006) was received on 03 April 2006. By this response, Claims 1, 8, 18, and 20 have been amended. Claims 3-7 have been canceled. No new claims have been added. Claims 1, 8-18, and 20 are currently pending in the present application.

Response to Arguments

2. Applicant's arguments filed 13 December 2005 and re-filed 03 April 2006 have been fully considered but they are not persuasive.

All pending claims were rejected under 35 U.S.C. 112, first paragraph, for failing to comply with the written description requirement; under 35 U.S.C. 112, second paragraph, as indefinite; and under 35 U.S.C. 103(a) as unpatentable over Menezes et al, *Handbook of Applied Cryptography*.

3. The rejection under 35 U.S.C. 112, first paragraph, has been rendered moot by the amendments to the independent claims. The rejection under 35 U.S.C. 112, second paragraph, regarding the limitation "wherein an update of a key distribution center database is, at least in part, capable of being avoided when at least one of the nodes is unfamiliar" has similarly been rendered moot by the amendments made removing the phrase "at least in part" from the limitation.

4. However, the rejection due to indefiniteness under 35 U.S.C. 112, second paragraph, specifically in reference to the claimed limitations of "verifying the hash value" is maintained. The Examiner notes that a response to Applicant's arguments regarding this ground of rejection was provided in the Notice of Non-Compliant Amendment mailed 03 March 2006. Because Applicant has opted not to respond further to the Examiner's response, the Examiner's arguments will be repeated herein for convenience:

Regarding the rejections of Claims 1, 8, 11, 18, and 20 under 35 U.S.C. 112, second paragraph, specifically in reference to the claimed limitations of "verifying the hash value", Applicant again asserts that deletion of the language limiting the location of the hash values provides claim breadth; Applicant also asserts that Claim 8 has been "clarified" to overcome indefiniteness. Regarding the alleged clarification of Claim 8, and also the language of Claim 11, the Examiner believes that the limitations of "validating the hash value" in Claim 8 and "verifying the hash value" in Claim 11 **still render the claims indefinite** because it is **not clear** whether these limitations refer to the first verification of the hash value (see Claim 1, page 3, line 5 of the present response) or to the second verification of the hash value (see Claim 1, page 3, line 13 of the present response).

Regarding Applicant's assertion that the removal of the limiting language provides claim breadth, Applicant further argues that the Examiner cited Figure 6 to assert that the locations of the hash verifications is vital to the functioning of the claimed protocol (see pages 12-13 of the present response). First, the Examiner notes that

Figure 6 itself was not cited as support, but rather all of the supporting description of Figure 6 at pages 13-16 of the specification, with specific reference to paragraphs 0061 and 0063 (see page 4 of the Office action mailed 20 September 2005); the Examiner additionally notes that Applicant cites the very same paragraphs at page 13 of the present response. Although the Examiner concedes that the specification does not explicitly disclose the locations of the hash verifications as "vital", the Examiner nevertheless **maintains** that omission of the locations of the hash verifications **renders the claims indefinite**. The Examiner notes that the locations of other functions are claimed (e.g. sending of messages from one location to another, recreating a key at the KDC, etc.); the Examiner again asserts that it is clear from the cited portion that one of the hash verifications takes place at the second node (page 15, paragraph 0061 of the present specification) and the other takes place at the first node (page 15, paragraph 0063). Therefore, because the claim recites locations for other operations performed and the specification details where the hash verifications are to be performed, the Examiner believes that omission of the locations of the hash verifications renders the claims indefinite. Further, because there is **no distinction drawn** between the two hash verifications, it is **impossible to determine** which hash verification is being referenced in Claim 1 (at page 3, line 16 of the present response), in Claim 18 (at page 7, line 26 of the present response), or further in dependent Claims 8 and 11 (as noted above).

Therefore, for the reasons detailed above, the Examiner maintains the rejections under 35 U.S.C. 112, second paragraph, as set forth below.

5. Regarding the rejection under 35 U.S.C. 103(a), first, although Applicant acknowledges that Menezes discloses key establishment (page 14 of the present response), Applicant still alleges that that "there is clearly not even a suggestion of any sort of 'key distribution center'" in Menezes (page 15 of the present response). The Examiner again notes that Menezes clearly states that the server in protocol 12.26 is a key distribution center (see page 497, Table 12.2, where the "server type" for the Needham-Schroeder protocol, later described as Protocol 12.26, is listed as "KDC"). The Examiner further notes that the allegation that Menezes does not disclose a key distribution center is at odds with Applicant's later assertion that the technique relied upon by Menezes (i.e. the Needham-Schroeder protocol) is analogous to Kerberos (see, for example, page 17 of the present response), which is another key establishment protocol having a key distribution center.

Applicant further argues that Menezes does not teach sending a second message from the second node to a key distribution center as claimed (page 15 of the present response). The Examiner notes that, in making this argument, Applicant refers to node A in Menezes as the first node and node B as the second. However, the Examiner notes that the previous Office actions mapped the second message, from the second node to the KDC, to "message 1" (Menezes, page 503, protocol 12.26; see also, for example, page 12 of the Office action mailed 20 September 2005); the Examiner wishes to clarify that this mapping was intended as mapping "node B" in Menezes to the claimed "first node" and similarly "node A" became the "second node" ("T" remained the key distribution center).

Applicant additionally argues, in response to the Examiner's previous remarks in the Office action mailed 20 September 2005 regarding the message authentication code (MAC), specifically that the second node and key distribution center share the second node key, that Applicant does not claim anywhere that the second node and key distribution center share a key (page 16 of the present response). However, the Examiner notes that if the second node key belongs to the second node (as claimed in Claim 1 at line 8 of the claim in the present response) and the second node key is further recreated at the key distribution center (Claim 1, line 9; also, as noted on page 16 of the present response), then both the second node and the key distribution center possess the key, and therefore share the key.

Further in response to the Examiner's previous remarks in the Office action mailed 20 September 2005 regarding the MAC being based on a secret key, and that the MAC is not itself a secret key, on page 16 of the present response, in the last paragraph, Applicant **misquotes** a cited portion of the Menezes reference. The insertion of the word "are" in the quoted phrase "[d]ata origin authentication mechanisms [are] based on shared secret keys (e.g. MACs)" (emphasis and bracketing Applicant's) **fundamentally alters** the meaning of the quoted section. In the original phrase "Data origin authentication mechanisms based on shared secret keys (e.g. MACs) do not allow" (original at Menezes, page 361, below Definition 9.77), it is clear that the parenthetical example of MACs is intended to modify the entire phrase "data origin authentication mechanisms based on shared secret keys" and not merely "shared secret keys" as asserted by Applicant. However, Applicant's manipulation of the quoted

portion by insertion of "are" would alter the meaning of the quoted section so that it appears that the parenthetical example of MACs modifies only "shared secret keys". It is clear that this is not the intended meaning of the cited portion.

The Examiner therefore respectfully disagrees with Applicant's assertion that "Menezes expressly discloses that MACs are an example of a shared secret key". In addition to the plain meaning of the unaltered cited portion, the Examiner believes that Menezes provides ample additional evidence that a MAC is **based on** a secret key. See, for example, page 33, the last paragraph of section 1.9, "Hash Functions" where MACs are described as "hash functions which involve a secret key"; also see page 360, Figure 9.8(a) where a secret key is an **input** to a MAC algorithm and a MAC is output. See also Schneier, *Applied Cryptography*, portions of which were cited in the Office action mailed 07 January 2005, noting, for example, page 31, under the heading "Message Authentication Codes", where a MAC "is a one-way hash function **with the addition of** a secret key".

However, the arguments addressed above notwithstanding, upon further consideration of the **claims as amended** and the **prior art** of record, the claims would be considered to be allowable if the claims were to be rewritten or amended to overcome the above-noted rejections under 35 U.S.C. 112, second paragraph. The Examiner notes that the claims are deemed to contain allowable subject matter **only** for the reasons set forth below under the heading "Allowable Subject Matter". The indication of allowable subject matter is not to be considered as acquiescence to any

specific arguments set forth by Applicant in the present or previous responses, but rather is based on consideration of the prosecution history **as a whole**.

Specification

6. The objection to the specification as failing to provide proper antecedent basis for the claimed subject matter is withdrawn in light of the amendments to the claims.

Claim Rejections - 35 USC § 112

7. The rejection of Claims 1, 8-18, and 20 under 35 U.S.C. 112, first paragraph, is withdrawn as noted above in light of the amendments to the claims.

8. The rejection of Claims 1, 8-18, and 20 under 35 U.S.C. 112, second paragraph, is maintained for the reasons noted above, and is again set forth below.

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1, 8-18, and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 18, and 20 each recite the limitation "verifying the hash value" twice (in Claim 1, see page 3, lines 5 and 13, of the present response; in Claim 18, see page 7,

lines 17 and 23; and in Claim 20, see page 9, lines 23 and 30, noting that the claim recites "to verify the hash value); however, it is not clear whether the verifications take place at the first node, the second node, or the key distribution center. Further, it is not clear whether references to verification of the hash value later in the claims (for example, in Claim 1, at page 3, line 16 "if the hash value is verified"; in Claim 8 "wherein validating the hash value includes"; in Claim 11 "wherein verifying the hash value includes"; and in Claim 18, page 7, line 26, "if the hash value is verified") are intended to refer to the first verification of the hash value or the second verification of the hash value. Because there is no distinction drawn, such as location, between the first and second hash value verifications in each of Claims 1, 18, and 20, this renders the claims indefinite.

For purposes of interpreting the prior art, it is assumed that the limitations are intended to read as follows: In Claim 1, the first instance (page 3, line 5) has been interpreted as reading "verifying the hash value at the second node", and the second instance (page 3, line 13) has been interpreted as reading "verifying the hash value at the first node". In Claim 18, the first instance (page 7, line 17) has been interpreted as reading "verifying the hash value at the second node", and the second instance (page 7, line 23) has been interpreted as reading "verifying the hash value at the first node". In Claim 20, the first instance (page 9, line 23) has been interpreted as reading "a second verifying mechanism that is configured to verify the hash value at the second node", and the second instance (page 9, line 30) has been interpreted as reading "a third verifying mechanism that is configured to verify the hash value at the first node".

Claim 8 recites the limitation "validating the hash value". There is insufficient antecedent basis for this limitation in the claims, as there is no explicit reference to validating or validation of a hash value in the claims. Further, if, as assumed, this is intended to refer to a *verification* of the hash value, then this is unclear as to which verification of a hash value in Claim 1 this is intended to refer, as noted above. For purposes of interpreting the prior art, it is assumed that this is intended to read "verifying the hash value at the second node".

Claim 11 recites the limitation "verifying the hash value"; however, as noted above, it is not clear whether this refers to the first verification of the hash value or the second verification of the hash value recited in Claim 1. For purposes of interpreting the prior art, it is assumed that this is intended to read "verifying the hash value at the first node".

All other claims not referred to above are rejected due to their dependence on a rejected base claim.

Allowable Subject Matter

11. Claims 1, 8-18, and 20 would be allowable if rewritten or amended to overcome the rejections under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

12. The following is a statement of reasons for the indication of allowable subject matter:

Independent Claims 1, 18, and 20 are directed to a method, apparatus, and software implementation of a method performing a cryptographic key establishment protocol. The protocol includes several messages sent between first and second nodes and a key distribution center. The protocol further includes node keys created based on node identifiers and secret knowledge, verification of message authentication codes based on the node keys, and verification of hash values of the identifiers combined with nonces. The protocol at its most basic level includes the first node requesting from the second node the establishment of a key, the second node requesting a key from the key distribution center (KDC), the KDC generating a shared key and sending the shared key to each node encrypted under the respective node keys, and the nodes establishing with each other that each node has the shared key by exchanging predetermined messages comprising hash values encrypted under the shared key. The closest prior art, Menezes et al, *Handbook of Applied Cryptography*, discloses a similar key distribution protocol, the Needham-Schroeder protocol, which also includes requesting establishment of a shared key from a KDC, the KDC generating the shared key and sending the shared key to each node encrypted with the respective node keys, and the nodes establishing that each has the shared key by exchanging messages encrypted under the shared key (page 503, protocol 12.26). Menezes further discloses identity-based key generation to prevent forgery and impersonation (page 561, section 13.4.3), the generation of message authentication codes to provide data origin authentication and data integrity (page 361, definition 9.77), and the generation of hash values as another means of providing data integrity (pages 321-322, section 9.1). However,

Menezes does not explicitly disclose or implicitly suggest exactly the steps of the protocol or the content of the messages as claimed in independent Claims 1, 18, and 20 (noting particularly the newly added limitations in the independent claims). Therefore, the claims contain subject matter allowable over the prior art of record.

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER